

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

JC872 U.S. PTO  
09/884427  
06/19/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 6月22日

出 願 番 号

Application Number:

特願2000-226083

出 願 人

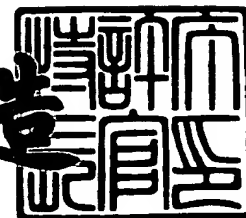
Applicant(s):

株式会社ビー・エス・ワイ

2001年 5月30日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3046471

【書類名】 特許願

【整理番号】 P2000-001

【提出日】 平成12年 6月22日

【あて先】 特許庁長官 殿

【発明者】

    【住所又は居所】 東京都台東区台東2丁目19番10号木村屋ビル3階

    【氏名】 王 志星

【特許出願人】

    【住所又は居所】 東京都台東区台東2丁目19番10号木村屋ビル3階

    【氏名又は名称】 株式会社ビー・エス・ワイ

    【代表者】 松岡 幸夫

    【電話番号】 03-3837-0401

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【書類名】 明細書

【発明の名称】 光の干渉原理に基づく暗号方式

【特許請求の範囲】

【請求項 1】 デジタル化の光信号（点光源）からある点 P において、2 本の光を干渉させ、暗号鍵を光信号の振幅、波長、初期位相および点 P に到達する光路差の初期値に変換し、2 つの光波の光路差を動的に変化させ、P 点で変化の干渉縞の明るさにおいて得られるデジタル化のデータを、入力された平文データに E O R（排他的論理和）し、平文データの内容を攪乱することを特徴とする光の干渉原理に基づく暗号方式とその暗号方式を使用する装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタル化された文書を高速伝送するためのデータ送信技術に係り、特に簡単な構成で安全な暗号データを発生させる技術に関する。

【0 0 0 2】

【従来の技術】

安全性の高い暗号方式としては D E S と R S A が知られており、これらは暗号処理の手段として最もよく使用されている。

【0 0 0 3】

【発明が解決しようとする課題】

しかしながら、D E S の暗号鍵の種類が多くとれないため、しらみつぶ式的に解読される危険性がある。また D E S の仕組みが複雑であり、演算速度が遅いという問題点がある。

【0 0 0 4】

【課題を解決するための手段】

上記の問題点を解決するために、本発明は、暗号鍵をデジタル化光信号（点光源）の振幅、波長、初期位相および光路差の初期値に変換することにより、暗号鍵の種類が多くとれる。また、光の干渉信号を発生する装置の仕組みが単純なため、暗号化及び復号化の演算速度が高速となることができる。

【0005】

## 【発明の実施の形態】

本発明は、デジタル化の光信号（点光源）からある点Pにおいて、2本の光を干渉させ、暗号鍵を光信号の振幅、波長、初期位相および点Pに到達する光路差の初期値に変換し、2つの光波の光路差を動的に変化させ、P点で変化の干渉縞の明るさにおいて得られるデジタル化のデータを、入力された平文データにEOR（排他的論理和）し、平文データの内容を攪乱させ、暗文データを出力する装置である。

【0006】

同じ振幅A、波長 $\lambda$ 、初期位相 $\phi_0$ の2本の光信号は、ある点Pに到達する光路差を $\Delta s$ とする。両波の行程に含まれる波の数の差は $\Delta s / \lambda$ 個である。両波で同じ位相であるから、P点に到達する2つの光波の位相差は、P点で

$$\Delta \phi = 2\pi * \Delta s / \lambda$$

になっている。よって、一例として、光波のP点における変位がそれぞれ

$$y_1 = A \sin(\omega t + 2\pi * \Delta s / \lambda + \phi_0) \text{ および}$$

$$y_2 = A \sin(\omega t - 2\pi * \Delta s / \lambda + \phi_0)$$

となる。ここで、Aは振幅、 $\omega$ は角速度、tは時刻、 $\Delta s$ は光路差、 $\lambda$ は波長、 $\phi_0$ は初期位相である。よって、両波の変位を合成すれば、

$$Y = y_1 + y_2$$

$$= A \sin(\omega t + 2\pi * \Delta s / \lambda + \phi_0) +$$

$$A \sin(\omega t - 2\pi * \Delta s / \lambda + \phi_0)$$

$$= 2A \sin((2\omega t + 2\phi_0) / 2) \cos((2\pi * \Delta s / \lambda) / 2)$$

$$= 2A \cos(\pi * \Delta s / \lambda) \sin(\omega t + \phi_0)$$

ここで、時刻 $t = 0$ における変位と光路差の関係を示す式は、

$$Y = 2A \cos(\pi * \Delta s / \lambda) \sin(\phi_0)$$

P点での明るさIはP点での波動エネルギーに比例するから、

$$I \propto 2A \cos(\pi * \Delta s / \lambda) \sin(\phi_0)$$

$$I = I_0 \cos(\pi * \Delta s / \lambda) \sin(\phi_0)$$

ここで、 $I_0$ は係数である。

## 【0007】

よって、係数  $I_0$  を  $a$ 、光路差  $\Delta s$  を  $x$  とすれば、 $P$  点における干渉縞の明るさは、下記の関数式で示すことができる。

$$f(x) = a * \cos(\pi * x / \lambda) * \sin(\phi_0)$$

前回の状態から逐次的に次の状態を計算するために、関数式

$$x_{n+1} = f(x_n) = a * \cos(\pi * x_n / \lambda) * \sin(\phi_0)$$

$$n = 0, 1, 2, \dots$$

が得られる。暗号鍵を光信号の振幅  $a$ 、波長  $\lambda$ 、初期位相  $\phi_0$  および点  $P$  に到達する光路差の初期  $x_0$  に変換し、前回の状態から逐次的に次の状態を計算することにより、2つの光波の光路差  $x_n$  を動的に変化することができる。よって、 $P$  点における干渉縞の明るさ  $x_{n+1}$  は乱数系列  $x_1, x_2, x_3, \dots$  となる。

## 【0008】

暗号鍵の長さは128ビットと仮定し、32ビットで分割すると鍵系列  $K_1, K_2, K_3, K_4$  となる。鍵系列を光信号の振幅  $a$ 、波長  $\lambda$ 、初期位相  $\phi_0$  および  $P$  点に到達する光路差の初期値  $x_0$  の有効値に変換すれば

$$f_{K1}(K_1) = x_0, f_{K2}(K_2) = a, f_{K3}(K_3) = \lambda, f_{K4}(K_4) = \phi_0$$

となる。ここで、 $x_0, a, \lambda, \phi_0$  は浮動小数である。この変換により、 $f(x) = a * \cos(\pi * x / \lambda) * \sin(\phi_0)$  のパターン数は、 $2^{128}$  となる。

## 【0009】

平文データに乱数  $x$  をEOR（排他的論理和）して、平文内容を攪乱することができる。平文データのビット系列を  $m_1, m_2, \dots$ 、乱数のビット系列を  $x_1, x_2, \dots$  とすると、暗号文のビット系列  $c_1, c_2, \dots$  は

$$c_i = m_i \text{ EOR } x_i \quad (i = 1, 2, \dots)$$

で与えられる。このとき、復号側は同様の操作

$$m_i = c_i \text{ EOR } x_i \quad (i = 1, 2, \dots)$$

となる。

## 【0010】

## 【実施例】

実施例について図面を参照して説明すると、図2において、暗号鍵分割手段8で長さ128ビットの暗号鍵を32ビットで分割し、鍵 $K_1$ 、 $K_2$ 、 $K_3$ 、 $K_4$ となる。一実施例として、鍵変換装置1で、

$$f_{K_1}(K_1) = x_0, \quad 0.800000000000 < x_0 < 0.890000000000$$

$$f_{K_2}(K_2) = a, \quad 0.900000000000 < a < 0.990000000000$$

$$f_{K_3}(K_3) = \lambda, \quad 0.500000000000 < \lambda < 0.590000000000$$

$$f_{K_4}(K_4) = \phi_0, \quad 8.000000000000 < \phi_0 < 8.900000000000$$

のように各初期値に変換する。

## 【0011】

図3に示される実施例では、平文入力装置3でデータを読み取り、EOR回路（暗号データ発生装置4）に入力する。2は、光の干渉原理に基づいて光の干渉信号発生装置である。光路差の初期値 $x_0$ より、干渉縞の明るさは $x_1$ 、 $x_2$ 、 $\dots$ となって、前回の状態から逐次的に次の状態を計算することができる。光の干渉信号発生装置2から出力されるデータは、そのまま $x$ 記憶部9に入力させる一方、加算器11に入力させる。前回のデータは、フィードバック信号としてインバータ10および加算器11によって減算回路を構成してある。加算器11から出力されるデータは、EOR回路（暗号データ発生装置4）に入力させる。

## 【0012】

図4は、データの復号化手段を示すものである。図4に示すハード部品は基本的に図3に示したものと同様であるから、同一機能を果たす部分は同一符号を付して重複説明を省略する。図4に示される実施例では、通信回線5からデータを受信させ、EOR回路（暗号データ復号装置6）に入力させる。加算器11から出力されるデータは、EOR回路（暗号データ復号装置6）に入力させる。

## 【0013】

【発明の効果】

本発明は、以上説明したような形態で実施され、以下に記載されるような効果を奏する。

【0014】

暗号鍵を光信号の振幅、波長、初期位相および点Pに到達する光路差の初期値に変換することにより、暗号鍵の長さは128ビットとなって、暗号鍵の種類が多とることができる。

【0015】

また、光の干渉原理に基づいて光の干渉信号発生装置の仕組みが単純なため、暗号化及び復号化の演算速度が高速となることができる。

【図面の簡単な説明】

【図1】

本発明の原理構成図である。

【図2】

本発明の一実施例の鍵変換システムの構成図である。

【図3】

本発明の一実施例の暗号化システムの構成図である。

【図4】

本発明の一実施例の復号化システムの構成図である。

【符号の説明】

- 1 鍵変換装置
- 2 光の干渉信号発生装置
- 3 平文入力装置
- 4 暗号データ発生装置
- 5 通信回線
- 6 暗号データ復号装置
- 7 平文出力装置
- 8 暗号鍵分割手段
- 9 x記憶部

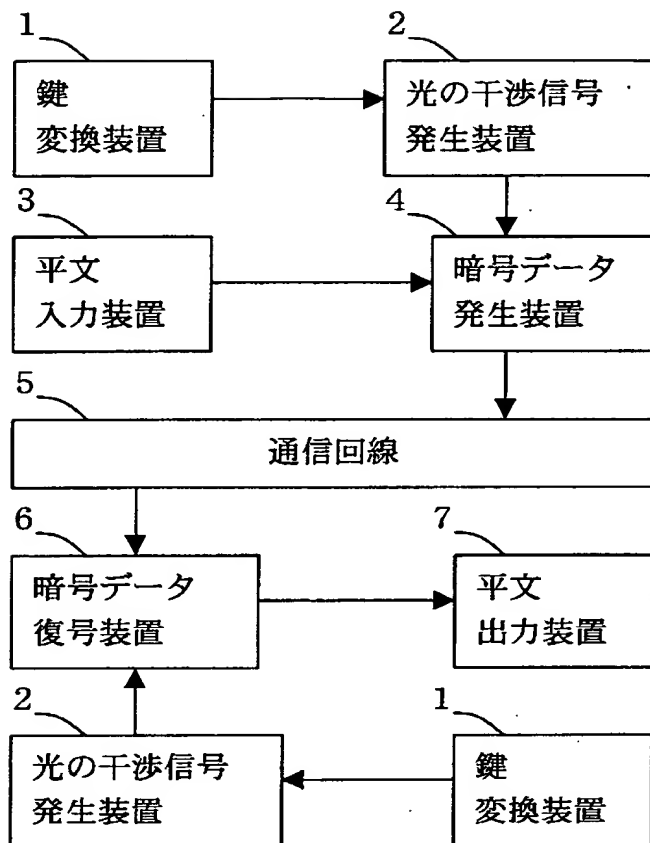
1 0    インバータ

1 1    加算器

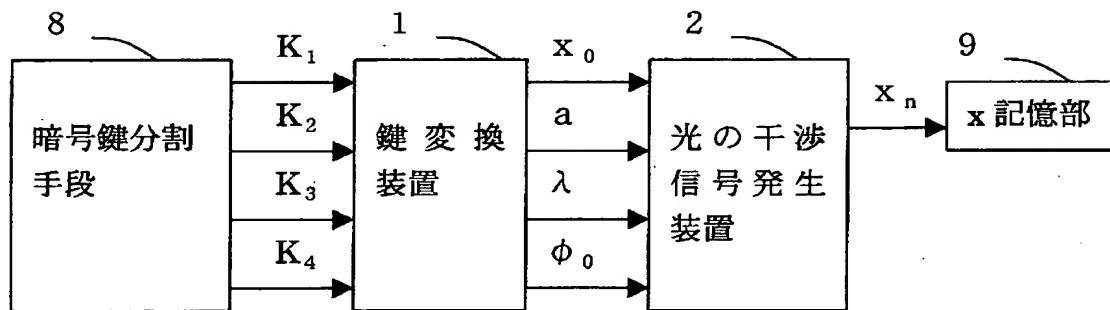


【書類名】 図面

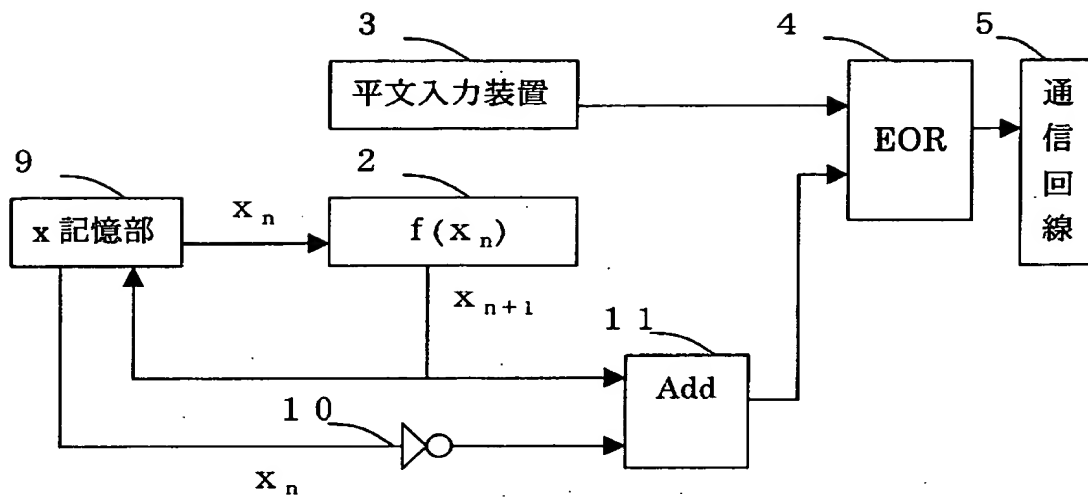
【図 1】



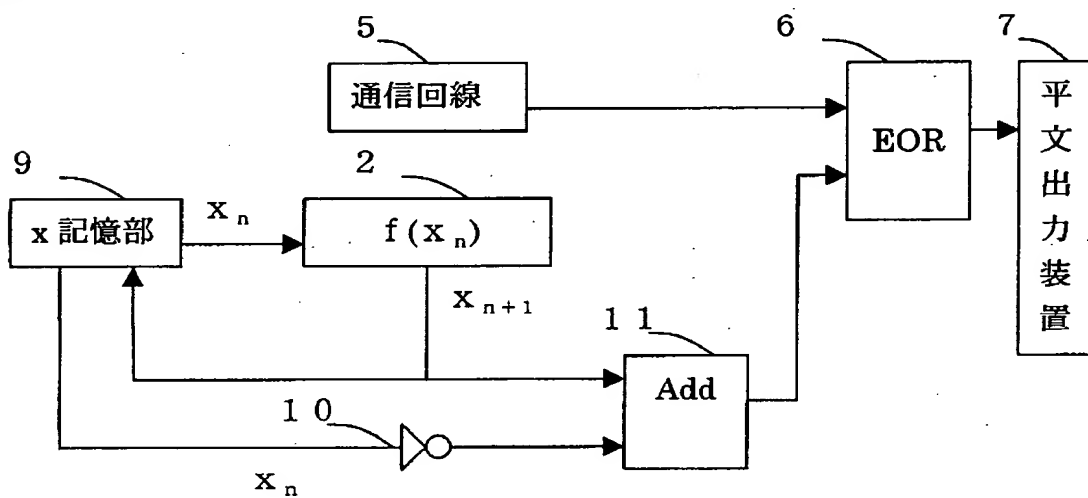
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 より高速かつ安全性を一層高めた光の干渉原理に基づく暗号方式を提供することである。

【解決手段】 デジタル化の光信号（点光源）からある点Pにおいて、2本の光を干渉させ、暗号鍵を光信号の振幅、波長、初期位相および点Pに到達する光路差の初期値に変換し、2つの光波の光路差を動的に変化させ、P点で変化の干渉縞の明るさにおいて得られるデジタル化のデータを、入力された平文データにEOR（排他的論理和）し、平文データの内容を攪乱する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [500346969]

1. 変更年月日 2000年 6月22日

[変更理由] 新規登録

住 所 東京都台東区台東2丁目19番10号 木村屋ビル3階  
氏 名 株式会社ビー・エス・ワイ